September 5, 2012

AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles, as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists". The Informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database six times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) or Mobile Digital Computer (MDC), prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server within seconds of the scans occurring. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Most mobile ALPR units do not have a "continuous" connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at the beginning and end of their shift to ensure they have the latest informational data available. If the ALPR system is integrated with an MDC, it is possible for the user to update their data via the unit's cellular connection in the field.

BOSS (Back Office System Server)

The BOSS server is where all the stored ALPR data resides. Within the server are the "hotlists," which are deployed and used to compare the license plates that are scanned by the ALPR cameras. The "hotlists" are maintained by the ASAP (Advanced Surveillance and Protection) Unit and are set-up to refresh automatically. There are a few cases which specific hotlists have been set-up for certain units and they have to be updated manually (most of these lists are covert hotlists and the user is not notified of the "hit"). The primary use of the server is for storage of the license plate data captured. Currently, we maintain approx. (2) years' worth of license plate data from all of our LASD ALPR cameras. Detectives and other investigative resources can utilize the BOSS database in searches for full or partial license plate information. Additionally, we have set-up links to query other LA County police agencies approx. 26 at this time, and are in the process of setting up and expanded ability to search other county law enforcement agencies with ALPR such as San Bernardino County Sheriff and Riverside County Sheriff.

Department Policies and Guidelines

There are no written guidelines as to how to use the data. The policy of how we use Department resources (data) is listed below. Keep in mind data is often used as a "lead" to glean further information on an active investigation that law enforcement handles.

Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

3-07/200.00 SHERIFF'S DATA NETWORK (SDN)

The Sheriff's Data Network (SDN) central hub is at the Sheriff's Headquarters Building and is under the administration of Data Systems Bureau.

The Sheriff's Data Network is a high speed network connecting all Sheriff's Department facilities and participating Los Angeles County municipal police departments. The SDN provides connectivity between desktop computers throughout the Department, as well as connection to other networks such as the Internet, LA Net, CLETS, and the Statewide Integrated Narcotics System. The SDN currently provides access to a wide range of applications, such as AJIS, LARCIS, CWS, CCHRS, RAPS, FMS, Cal Gangs (Formerly GREAT), CWTAPPS, JDIC and the Department's Intranet Server. For an up-to-date list of applications available on the Sheriff's Data Network, contact the Data Systems Bureau Help Desk.

3-07/210.00 PERMISSIBLE USE

The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Sheriff's Department employees and other authorized users shall adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.

Employees are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

3-07/220.00 PROHIBITIONS

Employees shall not add, alter, copy, damage, delete, move, modify, tamper with or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

- Devise or exclude any scheme or artifice to defraud, deceive, destroy or extort,
- Wrongfully control or obtain money, property, or data,
- Disrupt or cause the disruption of computer or network services, or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network,
- Assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

Unless specifically authorized by Data Systems Bureau, Department employees shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment or software.

Employees shall not do any of the following without the required authorization:

- Access or allow access to another to obtain, alter, or prevent access to stored electronic communications,
- Use electronic communications to capture or open electronic communications of another, or access files without permission of the owner,
- Damage hardware, software, or other communications equipment or interfere with functionality,
- Attempt to breach any security measures on any electronic communications system, or attempt to intercept any electronic communication transmission,
- Modify or delete any file, folder or system audit, security, or ownership records or time stamp with the intent to misrepresent true system audit records,
- Access the files belonging to another for non-business purposes,
- Use someone else's USERID, password or access another person's files, or retrieve stored communications without authorization,
- Modify the hardware or software configuration on any computer,
- Use electronic communications to transmit (upload) or receive (download):
    - Any communication violating any applicable laws, regulations, or policies,
    - Proprietary or confidential Department information,
    - Chain letters,
    - Material that would be offensive to a reasonable person.
- Transmit any electronic message in violation of file size restrictions,
- Use Department computer equipment or network to send or receive electronic communications for non-Department business,
- Use computers, networks, or electronic communications to infringe on the copyright or other intellectual property rights of the County or third parties,

- Send or receive commercial software in violation of its license agreement,
- Copy personal files, programs, or images into any Department computer without authorization from their unit commander,
- Send anonymous messages or represent themselves as someone else, real or fictional, or send messages or images which are defamatory, fraudulent, threatening, harassing, sexual or contain derogatory racial or religious content,
- Establish any hidden or misidentified links on any web page,
- Send or forward messages which have been altered in order to deceive the receiver as to the original content,
- Use Department computers, networks, software, or electronic communications for personal financial, commercial, political, or other personal use,
- Use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment,
- Use electronic communications in competition with commercial services to individuals or organizations outside the Department,
- Use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering,
- Give out employee personal information such as home address and/or telephone numbers.

3-07/220.20 CALIFORNIA DEPARTMENT OF JUSTICE ADMONISHMENT

- As an employee of the Los Angeles County Sheriff's Department, you may have access to confidential criminal record and/or Department of Motor Vehicles record information which is controlled by statute. Misuse of such information may adversely affect the individual's civil rights and violates the law. Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11140 - 11144 and 13301 - 13305 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. Penal Code Sections 11142 and 13303 state:
- "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."
- California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

Any employee who is responsible for such misuse is subject to disciplinary action. Violations of this law may also result in criminal and/or civil actions.

3-07/250.00 LASD USER AUTHORIZATION AND ACKNOWLEDGMENT OF POLICIES AND GUIDELINES

Employees will be responsible for reading and signing the Sheriff's Department "User Acknowledgment of Electronic Communications Policy" form before obtaining authorization to access the Sheriff's Data Network. The Department form requires a counter signature by the user's supervisor at the rank of sergeant or higher. An employee may request authorization to access the Sheriff's Data Network by submitting the request as described under the manual section entitled, Data Communications Management (section 3-07/230.00), and attaching the signed user acknowledgment form.

User Acknowledgment of Electronic Communications Policy

I understand that the Los Angeles County Sheriff's Department requires each user, who has access to automated data communications, be responsible for adhering to its electronic communications policy sections as set forth in the Manual of Policy and Procedures, section 3-07/200.10 through section 3-07/250.00 inclusive. I have received a copy of these sections of the Manual of Policy and Procedures.

I understand that I must not have an expectation of privacy when using County electronic communications and acknowledge that my electronic communications may be monitored at any time by authorized employees.

By signing this form, I agree to abide by all policies, including state statutes relating to electronic communications and use of information, and understand that I will be held accountable for my actions, and that disciplinary actions may result from not abiding by these policies. I also agree to give authorized persons, including supervisors, auditors, and investigators access to my equipment, software, and files at reasonable times for the purposes of investigating compliance.

User Name (PRINT) User Signature
Date

As a supervisor, by my signature, I acknowledge my responsibility to have provided the electronic communications policies, section 3-07/200.10 through section 3-07/250.00 inclusive, to the above user. I also acknowledge that I am responsible for ensuring that the above user, whom I supervise, has read and understands' this policy.

Supervisor's Name (PRINT) Supervisor's Signature
Date

* Attached is our Field Operations Directive as to how we utilize ALPR in the field *

We do not have user manuals for members of the Department. We train personnel in groups utilizing the train the trainer methodology. Both interfaces of the ALPR system are intuitive and do not require extensive training.

Retention is currently limited by the size of the data stored. As we expand the number of ALPR units, we additionally have to minimize the retention of the data we keep. Currently, we would prefer to retain data indefinitely but this will change if we cannot keep up with the increasing data storage requirements. There is no national or state mandate specifically for ALPR data retention (in California) and we have looked at similar standards, such as video, which is currently (2) years.

Sergeant John Gaw
LASD / Technical Services Division
Communications and Fleet Management Bureau (CFMB)
Advanced Surveillance and Protection Unit (ASAP)
12440 East Imperial Highway, #130
Norwalk, CA 90650
(562) 345-4476 / Office
jlgaw@lasd.org
asap@lasd.org
http://intranet.lasd.sheriff.sdn/intranet/announcements/ASAP/ASAP.shtml
www.comptonasap.com
http://www.lasd.org/sites/ASAP/index.html
http://www.youtube.com/user/LACountySheriff

Los Angeles County Sheriff's Department